Anomaly Detection Report

Model: autoencoder

Source File: orglog1.csv

Total Anomalies Found: 11

Anomaly #0 | Severity: High | Type: Session Hijacking (Score: 0.0635)

```
Log Details:
syslog_ts: Jan 28 09:00:00  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 28/Jan/2026:09:00:00 +0530  request: GET /utxLogin/login HTTP/1.1  status: 302  bytes: 249  response_time: 6  referer: -  user_agent: -
```

LLM Analysis:

The anomaly detected in the server log indicates a potential session hijacking attack where an unauthorized user may have taken control of a valid session.

Reason for Detection:

The anomaly features such as the unexpected status code (302), along with the presence of suspicious IP addresses and a redirect request, suggest a possible session hijacking attempt.

Anomaly #1 | Severity: High | Type: Data Exfiltration (Score: 0.0613)

```
Log Details:
syslog_ts: Jan 28 09:00:00  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 28/Jan/2026:09:00:00 +0530  request: GET / HTTP/1.1  status: 302  bytes: -  response_time: 1  referer: -  user_agent: -
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been accessed and transferred out of the system.

Reason for Detection:

The unusually low response time (1 second) for a request with a status code of 302 (redirect) and missing bytes information raises suspicion of data exfiltration activity.

Anomaly #2 | Severity: High | Type: Data Exfiltration (Score: 0.0979)

```
Log Details:
syslog_ts: Jan 27 22:51:42  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 27/Jan/2026:22:51:42 +0530  request: GET / HTTP/1.1  status: 302  bytes: -  response_time: 0  referer: -  user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-IN) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity.

Reason for Detection:

The anomaly features such as duration, size, and method indicate abnormal behavior that could be indicative of data being transferred out of the system.

Anomaly #3 | Severity: High | Type: Data Exfiltration (Score: 0.0979)

```
Log Details:
```

Anomaly Detection Report

```
syslog_ts: Jan 27 22:51:52 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 27/Jan/2026:22:51:52 +0530 request: GET / HTTP/1.1 status: 302 bytes: - response_time: 0 referer: - user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity.

Reason for Detection:

The unusually low response time (0 seconds) and the presence of anomalous features such as Duration and Size suggest that data may have been quickly extracted from the server.

Anomaly #4 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0613)

```
Log Details:
syslog_ts: Jan 27 22:51:52 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 27/Jan/2026:22:51:52 +0530 request: GET /utxHomeApp/redirectToHome HTTP/1.1 status: 302 bytes: - response_time: 1 referer: - user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly detected in the server log indicates a potential attack involving a suspicious user agent.

Reason for Detection:

The anomaly features Duration, Size, and Method_POST suggest unusual behavior in the request, combined with a Windows PowerShell user agent, which is commonly associated with malicious activities.

Anomaly #5 | Severity: High | Type: Data Exfiltration (Score: 0.0979)

```
Log Details:
syslog_ts: Jan 27 22:51:56 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 27/Jan/2026:22:51:56 +0530 request: GET / HTTP/1.1 status: 302 bytes: - response_time: 0 referer: - user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, as the response time is unusually low and the size of the request is also small.

Reason for Detection:

The anomaly features Duration and Size have values significantly different from the norm, suggesting a potential data exfiltration attempt where a small amount of data was quickly transferred out of the server.

Anomaly #6 | Severity: High | Type: Data Exfiltration (Score: 0.0613)

```
Log Details:
syslog_ts: Jan 24 14:14:28 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 24/Jan/2026:14:14:28 +0530 request: GET /boardwebapp/company/ HTTP/1.1 status: 302 bytes: - response_time: 1 referer: - user_agent: curl/8.4.0
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been accessed and transferred out of the system.

Reason for Detection:

The anomalous features Duration, Size, and Method_POST suggest that a large amount of data was quickly transferred using a POST request, which is indicative of data exfiltration.

Anomaly Detection Report

Anomaly #7 | Severity: Medium | Type: Redirect to Home Page Attack (Score: 0.0613)

Log Details:

```
syslog_ts: Jan 27 22:52:41 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 27/Jan/2026:22:52:41 +0530 request: GET /utxHomeApp/redirectToHome HTTP/1.1 status: 302 bytes: - response_time: 1 referer: - user_agent: -
```

LLM Analysis:

This log anomaly indicates a potential attack where the server is redirecting users to the home page without proper authorization.

Reason for Detection:

The anomaly in the log details shows a redirect request with a status code of 302 and a very low response time, which is suspicious behavior and could indicate an attempt to bypass security measures.

Anomaly #8 | Severity: Medium | Type: Suspicious User Agent (Score: 0.0158)

Log Details:

```
syslog_ts: Jan 24 14:23:26 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 12345 domain: abc.example.net apache_ts: 24/Jan/2026:14:23:26 +0530 request: GET /agmipad/ HTTP/1.1 status: 302 bytes: - response_time: 13 referer: - user_agent: curl/8.4.0
```

LLM Analysis:

The anomaly detected in the server log indicates a potential suspicious user agent activity.

Reason for Detection:

The user agent 'curl/8.4.0' in the log entry is uncommon and could be indicative of a malicious actor attempting to access the server.

Anomaly #9 | Severity: High | Type: Directory Traversal (Score: 0.0021)

Log Details:

```
syslog_ts: Jan 28 12:52:40 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 559541 domain: projectcommercials-uat.test.company.net apache_ts: 28/Jan/2026:12:52:39 +0530 request: GET /pAccounting/appResources/js/angular/controller/fcm/fcmSupportController.js?v=/../../../../../../../../bin/id%00| HTTP/1.1 status: 200 bytes: 2202 response_time: 1148 referer: https://projectcommercials-uat.test.company.net/pAccounting/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
```

LLM Analysis:

The anomaly detected in the server log indicates a potential Directory Traversal attack where the attacker is trying to access sensitive system files by manipulating the file path in the request.

Reason for Detection:

The presence of multiple '../' in the request path 'GET /pAccounting/appResources/js/angular/controller/fcm/fcmSupportController.js?v=/../../../../../../../../bin/id%00|' is a clear indicator of a Directory Traversal attempt, triggering the anomaly detection.

Anomaly #10 | Severity: High | Type: Directory Traversal (Score: 0.0006)

Log Details:

```
syslog_ts: Jan 28 12:40:35 host: servernameabc process: httpd[12345] ip1: 0.0.0.0 ip2: 0.1.0.1 session_id: 559541 domain: projectcommercials-uat.test.company.net apache_ts: 28/Jan/2026:12:40:35 +0530 request: GET /pAccounting/extResources/tooltip/tipsy-docs.js?v=/../..//../../..//../../..//../../..//../../..//../..//etc/passwd%00 HTTP/1.1 status: 200 bytes: 931 response_time: 5 referer: https://projectcommercials-uat.test.company.net/pAccounting/index.html user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
```

LLM Analysis:

The server log anomaly indicates a potential Directory Traversal attack where the attacker attempted to access sensitive system files

by manipulating the file path in the request.

Reason for Detection:

The request 'GET /pAccounting/extResources/tooltip/tipsy-docs.js?v=/../..//../../..//../..//../../..//../../..//../..////etc/passwd%00 HTTP/1.1' contains multiple '../' sequences which is a common technique used in Directory Traversal attacks.
